PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 12/14

A1

(11) International Publication Number: **WO 00/52583**

(43) International Publication Date: 8 September 2000 (08.09.00)

(21) International Application Number: PCT/US99/31314

(22) International Filing Date: 29 December 1999 (29.12.99)

(30) Priority Data:
09/261,055 2 March 1999 (02.03.99) US

(71) Applicant *(for all designated States except US)*: AUDIBLE, INC. [US/US]; 65 Willowbrook Boulevard, Wayne, NJ 07470 (US).

(72) Inventor: HUFFMAN, Andrew, J. (deceased).

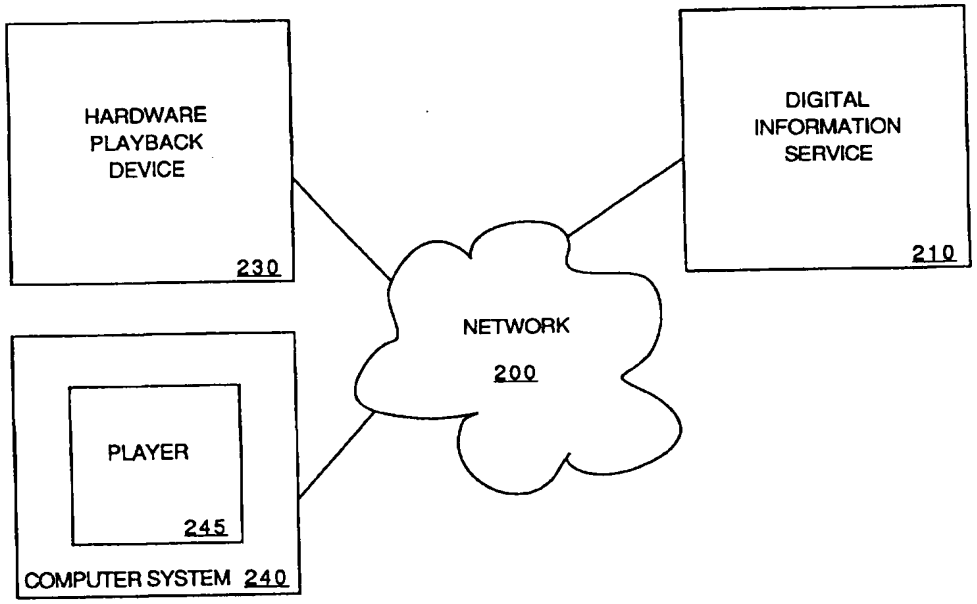
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: RAJASEKHARAN, Ajit, V. [IN/US]; 6 Lake Avenue, Apt. 6B, East Brunswick, NJ 08816 (US). STORY, Guy, A., Jr. [US/US]; 151 Spring Street, New York, NY 10012 (US).

(74) Agents: MILLIKEN, Darren, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE STREAMING OF DIGITAL AUDIO/VISUAL CONTENT



(57) Abstract

A method and apparatus for secure streaming of digital audio and/or visual content (210) is described. Authorization data corresponding to the digital content (210) is received. A check is performed to determine whether a playback device (230) is authorized to play the digital content (210) based, at least in part, on the authorization data. A stream of data representing portions of the digital content (210) is played, if authorized. In one embodiment, portions of the stream of digital content (210) are intermittently checked for authorization.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SECURE STREAMING OF DIGITAL AUDIO/VISUAL CONTENT

FIELD OF THE INVENTION

The invention relates to digital information playback. More particularly, the invention relates to secure streaming of digital information between a source and a playback device.

BACKGROUND OF THE INVENTION

Sources currently exist that provide digital audio and/or video content to remote playback devices. The digital content can be provided by a network, such as the Internet, or other network. The digital content can be provided as a file that is downloaded and played, or as a stream of data that can be played as received. For digital content that is subject to a controlled distribution, a security scheme is required.

One scheme for content protection is to protect access to the content. Access protection can be applied to both files and streams of content. For example, a user name and password may be required to access the content. However, access protection can be defeated, for example, by disclosure of a user name and/or password, or by otherwise determining an authorized user name and password. Once an authorized user name and password are obtained, an unauthorized party can have access to the content.

Because access protection can be defeated as described above, additional and/or different content protection schemes are often necessary to provide satisfactory content protection. Therefore, what is needed is a protection scheme that provided better content protection than simple content access protection.

SUMMARY OF THE INVENTION

A method and apparatus for secure steaming of digital audio and/or visual content is described. Authorization data corresponding the digital content is received. A check is performed to determine whether a playback device is authorized to play the digital content based, at least in part, on the authorization data. A stream of data representing portions of the digital content is played , if authorized. In one embodiment, portions of the stream of digital content are intermittently checked for authorization.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated by way of example, and not by way of limitation in the figures of the accompanying drawings in which like reference numerals refer to similar elements.

Figure 1 is one embodiment of a computer system suitable for use with the invention.

Figure 2 is one embodiment of an architecture that provides digital information for playback suitable for use with the invention.

Figure 3 is one embodiment of a computer system running a digital information player suitable for use with the invention.

Figure 4 is a flow diagram for providing secure streaming of digital content according to one embodiment of the invention.

Figure 5 illustrates authorization data for use in providing secure streaming digital content according to one embodiment of the invention.

DETAILED DESCRIPTION

A method and apparatus for secure streaming of digital audio/visual content is described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough

understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

The invention provides a method and apparatus for allowing secure streaming of digital audio/visual content. Secure streaming provides protection against unauthorized use of the digital content. Authorization and integrity checks are performed by a client or playback device on a set of data associated with digital content to be played. The set of data includes authorization and integrity information for content to be received from the source. Streamed content is received from the source by the playback device. The streamed content is intermittently checked for authorization and integrity. If the check is passed, playback continues; otherwise playback is halted.

Overview of an Architecture and Devices for Providing Playback of Digital Programming

Figure 1 is one embodiment of a computer system suitable for use with the invention. Computer system 100 includes bus 101 or other communication device for communicating information, and processor 102 coupled to bus 101 for processing information. While computer system 100 is illustrated with a single processor, computer system 100 can include multiple processors. Computer system 100 further includes random access memory (RAM) or other dynamic storage device 104 (referred to as main memory), coupled to bus 101 for storing information and instructions to be executed by processor 102. Main memory 104

also can be used for storing temporary variables or other intermediate information during execution of instructions by processor 102. Computer system 100 also includes read only memory (ROM) and/or other static storage device 106 coupled to bus 101 for storing static information and instructions for processor 102. Data storage device 107 is coupled to bus 101 for storing information and instructions.

Data storage device 107 such as a magnetic disk or optical disc and its corresponding drive can be coupled to computer system 100. Computer system 100 can also be coupled via bus 101 to display device 121, such as a cathode ray tube (CRT) or liquid crystal display (LCD), for displaying information to a computer user. Alphanumeric input device 122, including alphanumeric and other keys, is typically coupled to bus 101 for communicating information and command selections to processor 102. Another type of user input device is cursor control 123, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 102 and for controlling cursor movement on display 121.

In one embodiment, computer system 100 further includes playback device interface 130 that provides a communications interface between computer system 100 and a mobile playback device (not shown in Figure 1). Playback device interface 130 can be, for example, a docking station coupled to a port (not shown in Figure 1) of computer system 100 (e.g., serial port, parallel port, SCSI interface). The docking station is configured to receive a mobile playback device. Playback device interface 130 allows computer system 100 to communicate licensing information, digital content, and other data to and receive data from a mobile playback device.

In one embodiment, the invention is related to the use of computer system 100 to provide secure streaming digital content playback devices. According to one embodiment, secure streaming is provided by a computer system, such as computer system 100, in response to processor 102 executing sequences of instructions contained in memory 104.

Instructions are provided to main memory 104 from a storage device, such as magnetic disk, CD-ROM, DVD, via a remote connection (e.g., over a network), etc. In alternative embodiments, hard-wired circuitry can be used in place of or in combination with software instructions to implement the invention. Thus, the invention is not limited to any specific combination of hardware circuitry and software.

Figure 2 is one embodiment of an architecture that provides digital information for playback suitable for use with the invention. Server 210 is coupled to multiple playback devices, including hardware playback devices (e.g., 230) and players (e.g., 245 running on computer system 240), by network 200. Any number of hardware playback devices and players can be coupled to server 210 by network 200.

In one embodiment, network 200 is the Internet; however, other networks can be used. For example, network 200 can be an intranet that couples only computer systems and other devices together that belong to a particular organization. Network 200 can also represent a group of networks, such and a group of local area networks.

Server 210 stores digital information defining programming as well as information about authorized users of the digital information. In one embodiment, server 210 stores a library of digital content that can be accessed by authorized playback devices. The library of digital content can include audio books, recordings of lecture series, news, plays, movies, etc.

Hardware playback device 230 stores programs from server 210 for playback. Hardware playback device 230 can store all or a portion of one or more programs. Also, hardware playback device 230 can be coupled to network 200 directly or by a computer system (not shown in Figure 2) that accesses server 210. Computer system 240 runs player 245 and can play digital content from server 210.

Figure 3 is one embodiment of a computer system running a digital information player suitable for use with the invention. Processor 102 executes sequences of instruction stored in main memory 104 including sequences of instructions defining operating system 300 and player 310.

Main memory 104 further includes digital content 320 that is all or a portion of programming received from the server. Additional programs, or additional portions of digital content 320, can be stored by storage device 107 and copied to main memory 104 as necessary. For streaming digital content, only a portion of the digital content being played is stored in main memory 104.

Processor 102 retrieves data from digital content 320 and outputs audio and/or video in response to the data. Processor 102 can also retrieve digital content data from a network connection (not shown in Figure 3) for playback or for storage in main memory 104.

Overview of Secure Streaming of Digital Content

Figure 4 is a flow diagram for providing secure streaming of digital content according to one embodiment of the invention. The data can be audio data, visual data, or a combination of audio and visual data. The data can be played by a software player running on a computer system or other suitable device, or the data can be played by a dedicated hardware playback device.

Authorization data is received from a source at 400. In one embodiment, the source is a server computer system accessed via a network, such as the Internet. The server can provide the digital content as well as the authorization data, or the digital content can be received from a different source, or multiple sources. One embodiment of authorization data is described in greater detail below with respect to Figure 5.

In one embodiment, the authorization data includes one or more digital signatures, one or more user identifiers and one or more content integrity values. Other and/or different authorization data can also be used. The one or more

digital signatures allow the playback device to determine the authority of the source of the authorization data. The one or more user identifiers allow the playback device to determine whether the playback device is authorized to play the associated digital content. The content integrity values allow the playback device to determine whether the digital content is valid.

The playback device checks the authorization data at 410. In one embodiment, the playback device checks the digital signature, or other source indicator, in the authorization data to determine whether the authorization data is received from an authorized source. The digital signature can be, for example, either a Digital Signature Algorithm (DSA) signature as proposed by the National Institute of Standards, or a Rivest Shamir Adleman (RSA) algorithm as described by RSA Data Security, Inc. of Redwood City California. Both of these functions are described in pages 466-494 of "Applied Cryptography: Protocols, Algorithms and Source Code in C" by Bruce Schneier, published by John Wiley & Sons, Inc. (1996). Other signature algorithms can also be used.

The playback device determines whether it in an authorized playback device at 420. In one embodiment, the playback device has a PlayerID value. The PlayerID value can be received via a registration process, which is described in greater detail in U.S. Patent application 09/151,384, filed September 10, 1998, entitled "CLONING PROTECTION SCHEME FOR A DIGITAL INFORMATION PLAYBACK DEVICE," which is assigned to the corporate assignee of the invention. The PlayerID value can also be hardwired into, or otherwise provided by, a component of the playback device (e.g., a computer system, a hardware player).

If the playback device is not an authorized playback device at 420, the process stops. Otherwise, a stream of digital information is received and played at 430. In one embodiment, the stream of digital data is received form the same source as the authorization data; however, the digital data can be received from an alternative source.

In one embodiment, the playback device performs a periodic check of the stream of digital information at 440. The check can be performed at regular intervals (e.g., every 20 seconds), the check can be performed at random times, or the check can be performed at varying times within predetermined timing intervals. When performing checks at regular intervals conditions such as, for example, network bandwidth, processing power and strength of security desired, can be used to determine the interval to be used.

In one embodiment, the playback device generates a hash value based on a block of content received. The playback device checks the content integrity values previously received as part of the authorization data to determine whether the hash value is included. Content integrity values other than hash values can also be used.

If the check performed at 440 passes at 450, digital information playback is continued (e.g., 430, 440, 450). If the check fails at 450, playback of digital information is stopped. Thus, an unauthorized user can play a portion (e.g., 20 seconds) of unauthorized digital content, but the unauthorized user is prevented from continuing to play the stream of digital information.

Thus, the invention provides playback protection rather than access protection. In other words, the invention allows only authorized playback devices to play content that has been received. In contrast, access protection schemes attempt to limit access to the content that can be played by any playback device having access to the content. In providing playback protection, the invention allows greater protection to identification and authorization information as compared to access protection because authorization activities occur within the playback device rather than being distributed across a network where private information can be lost, stolen and/or sabotaged.

Figure 5 illustrates authorization data for use in providing secure streaming digital content according to one embodiment of the invention. In general, authorization data 500 includes source identifier 510, user identifiers 520

and content integrity values 530. Additional and/or different data can be used to provide authorization information.

In one embodiment, source indicator 510 is a digital signature corresponding to the source of authorization data 500. Source indicator 510 can also be multiple digital signatures indicating a chain of authorized sources through which the authorization data 500 has been received. Playback devices perform necessary checks on source indicator 510 to determine whether authorization data 500 is valid.

In one embodiment, user identifiers 520 include one or more PlayerID values corresponding to playback devices that are authorized to play the digital information with which authorization data 500 is associated. User identifiers 520 can also include GroupID values that correspond to groups of playback devices authorized to play the digital information. Playback devices determine whether a PlayerID or GroupID value linked to the playback device is included in user identifiers 520.

In one embodiment, content integrity values 530 are hash values corresponding to one or more portions of the digital content corresponding to authorization data 500. Content integrity values 530 are used by the playback device to determine whether the corresponding portion of digital content is valid. Content integrity values 530 are used for periodic checking by the playback device to determine whether playback is authorized.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes can be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method comprising:

receiving authorization data corresponding to streamed digital content;

determining whether a playback device is authorized to play the streamed digital content based, at least in part, on the authorization data; and

playing a portion of the streamed digital content, if authorized.

2. The method of claim 1 further comprising intermittently checking portions of the streamed digital content to determine whether continued playback is authorized.

3. The method of claim 2 wherein the intermittent checking is performed at regular intervals.

4. The method of claim 2 wherein the intermittent checking is performed randomly.

5. The method of claim 2 wherein the intermittent checking comprises:

determining a hash value for a portion of the steamed digital content;

checking the authorization data to determine whether the hash value is included; and

continuing playback if the hash value is included in the authorization data.

6. The method of claim 1 further comprising repeating determining whether the playback device is authorized to play the streamed digital content and playing a portion of the streamed digital content, if authorized.

7. The method of claim 1 wherein determining whether a playback device is authorized to play the digital content further comprises:

determining whether a source indicator included in the authorization data indicates an approved source; and

determining whether an authorization indicator in the authorization data corresponds to the playback device.

8. The method of claim 7 wherein the source indicator is a digital signature.

9. The method of claim 7 wherein the authorization indicator is a playback device indicator.

10. An apparatus comprising:

means for receiving authorization data corresponding to streamed digital content;

means for determining whether a playback device is authorized to play the streamed digital content based, at least in part, on the authorization data; and

means for playing a portion of the streamed digital content, if authorized.

11. The apparatus of claim 10 further comprising means for intermittently checking portions of the streamed digital content to determine whether playback is authorized.

12. The apparatus of claim 11 wherein the intermittent checking further comprises:

means for determining a hash value for a portion of the stream of data;

means for checking the authorization data to determine whether the hash value is included; and

means for continuing playback if the hash value is included in the authorization data.

13. The apparatus of claim 10 wherein the means for determining whether a playback device is authorized to play the digital content further comprises:

means for determining whether a source indicator included in the authorization data indicates an approved source; and

means for determining whether an authorization indicator in the authorization data corresponds to the playback device.

14. A machine-readable medium having stored thereon sequences of instructions what when executed by one or more processors cause an electronic device to to:

receive authorization data corresponding to streamed digital content;

determine whether a playback device is authorized to play the streamed digital content based, at least in part, on the authorization data; and

play a portion of the streamed digital content, if authorized.

15. The machine-readable medium of claim 14 further comprising intermittently checking portions of the streamed digital content to determine whether playback is authorized.

16. The machine-readable medium of claim 15 wherein the intermittent checking is performed at regular intervals.

17. The machine-readable medium of claim 15 wherein the intermittent checking is performed randomly.

18. The machine-readable medium of claim 15 wherein the sequences of instructions that cause the electronic device to intermittently check portions of the stream of data further comprise sequences of instructions that when executed by the one or more processors cause the electronic device to:

determine a hash value for a portion of the stream of data;

check the authorization data to determine whether the hash value is included; and

continue playback if the hash value is included in the authorization data.

19. The machine-readable medium of claim 14 wherein the sequences of instructions that cause the electronic device to play the portion of the digital content comprises receiving a stream of portions of a digital content file.

20. The machine-readable medium of claim 14 wherein the sequences of instructions that cause the electronic device to determine whether a playback device is authorized to play the digital content comprise sequences of instructions that when executed cause the electronic device to:

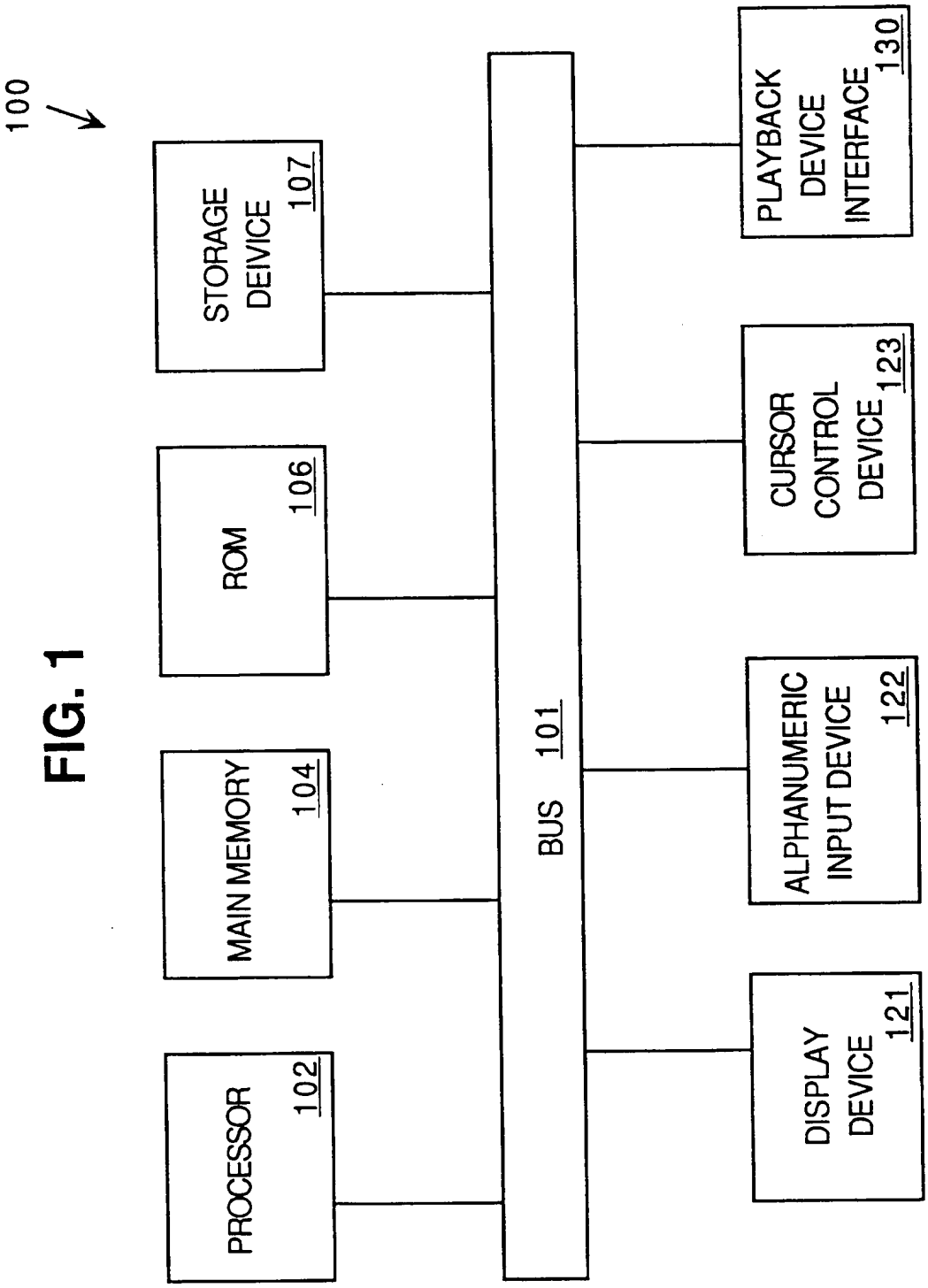
determine whether a source indicator included in the authorization data indicates an approved source; and

determine whether an authorization indicator in the authorization data corresponds to the playback device.

21. The machine-readable medium of claim 20 wherein the source indicator is a digital signature.

22. The machine-readable medium of claim 20 wherein the authorization indicator is a playback device indicator.

FIG. 1


100
PROCESSOR 102
MAIN MEMORY 104
ROM 106
STORAGE DEIVICE 107
BUS 101
DISPLAY DEVICE 121
ALPHANUMERIC INPUT DEVICE 122
CURSOR CONTROL DEVICE 123
PLAYBACK DEVICE INTERFACE 130

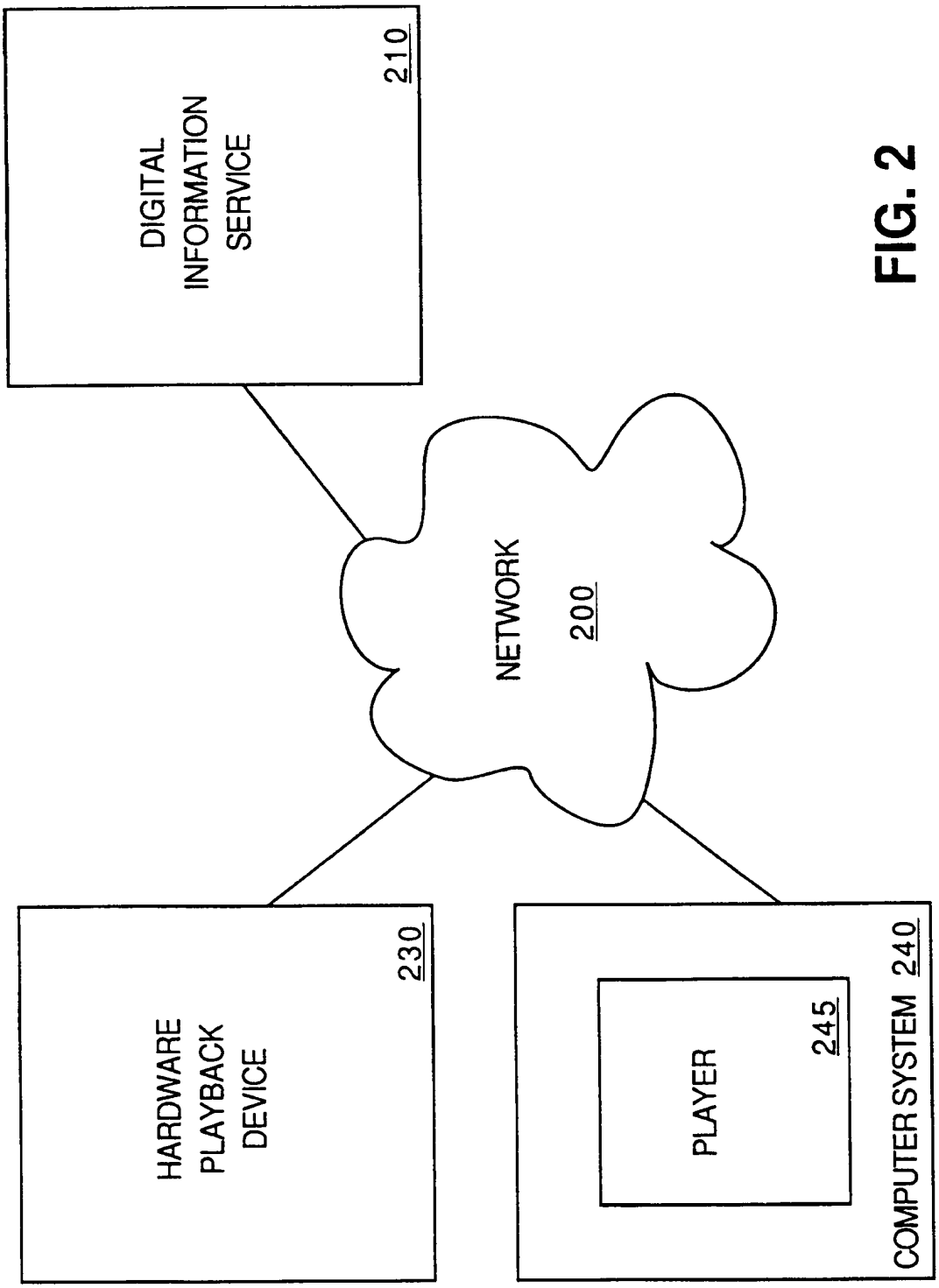

DIGITAL INFORMATION SERVICE
210
NETWORK
200
HARDWARE PLAYBACK DEVICE
230
COMPUTER SYSTEM 240
PLAYER
245

FIG. 2

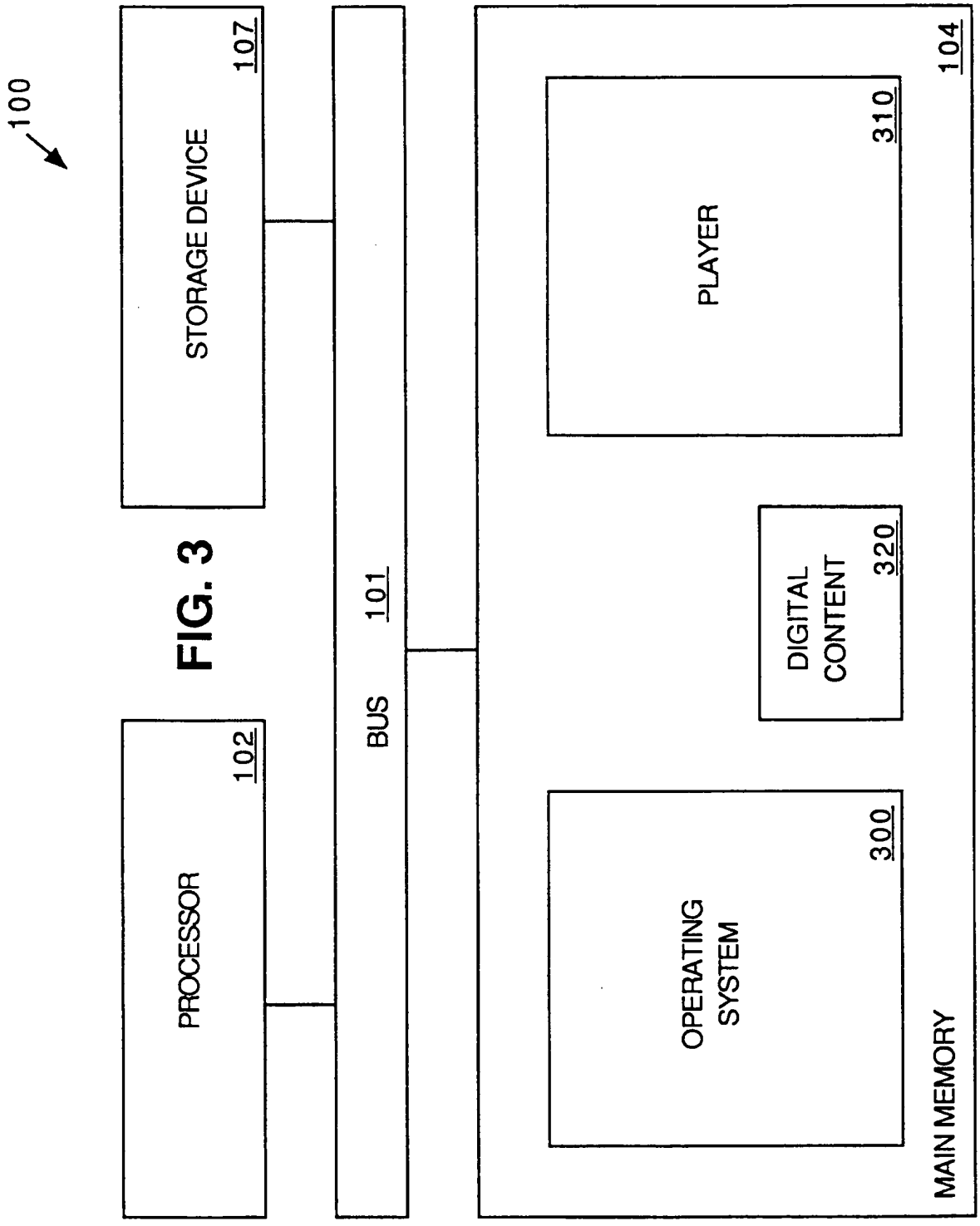

100
STORAGE DEVICE
107
PROCESSOR
102
BUS
101
MAIN MEMORY
104
PLAYER
310
DIGITAL CONTENT
320
OPERATING SYSTEM
300

FIG. 3

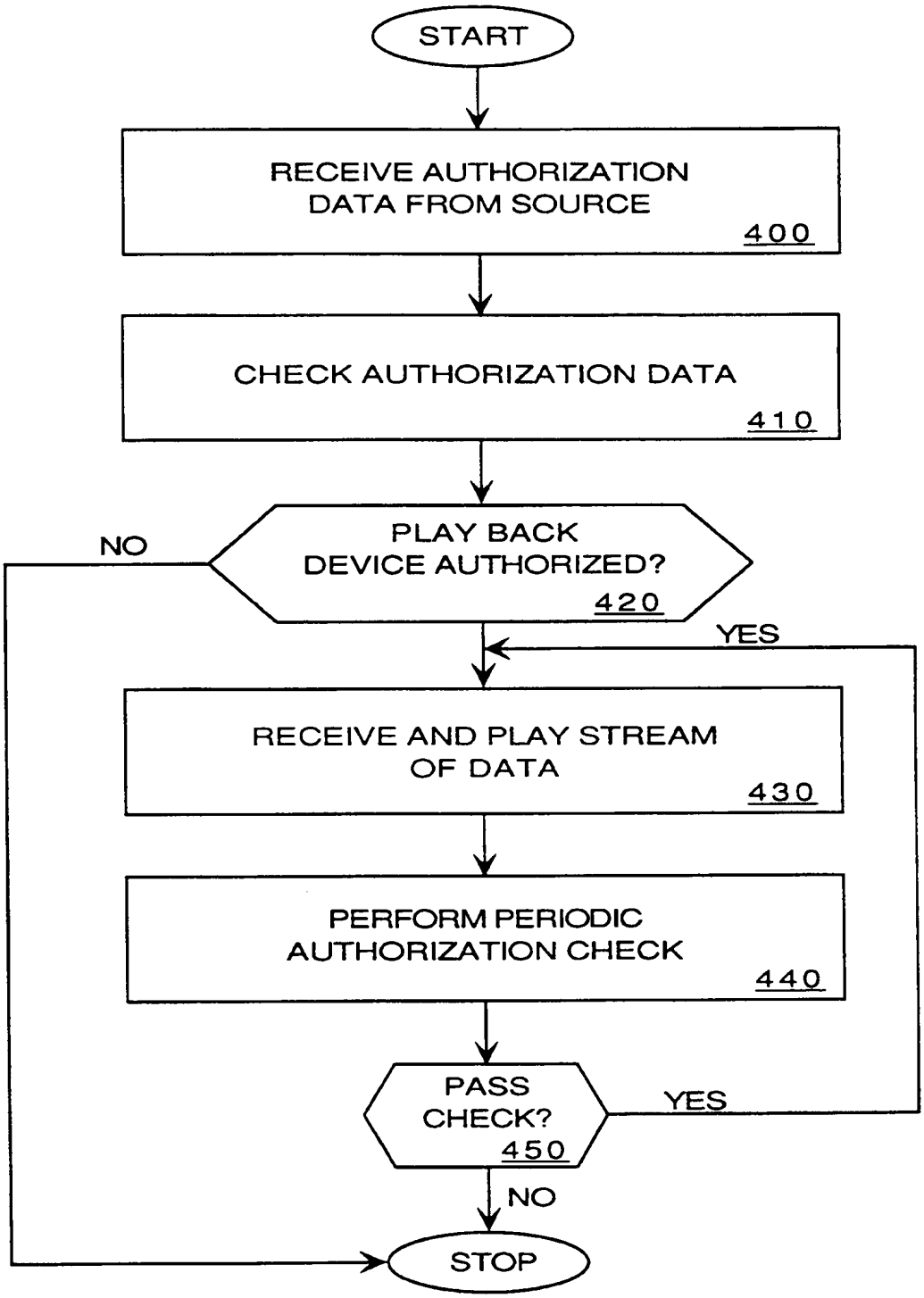

START
RECEIVE AUTHORIZATION DATA FROM SOURCE
400
CHECK AUTHORIZATION DATA
410
PLAY BACK DEVICE AUTHORIZED?
420
NO
YES
RECEIVE AND PLAY STREAM OF DATA
430
PERFORM PERIODIC AUTHORIZATION CHECK
440
PASS CHECK?
450
YES
NO
STOP

FIG. 4

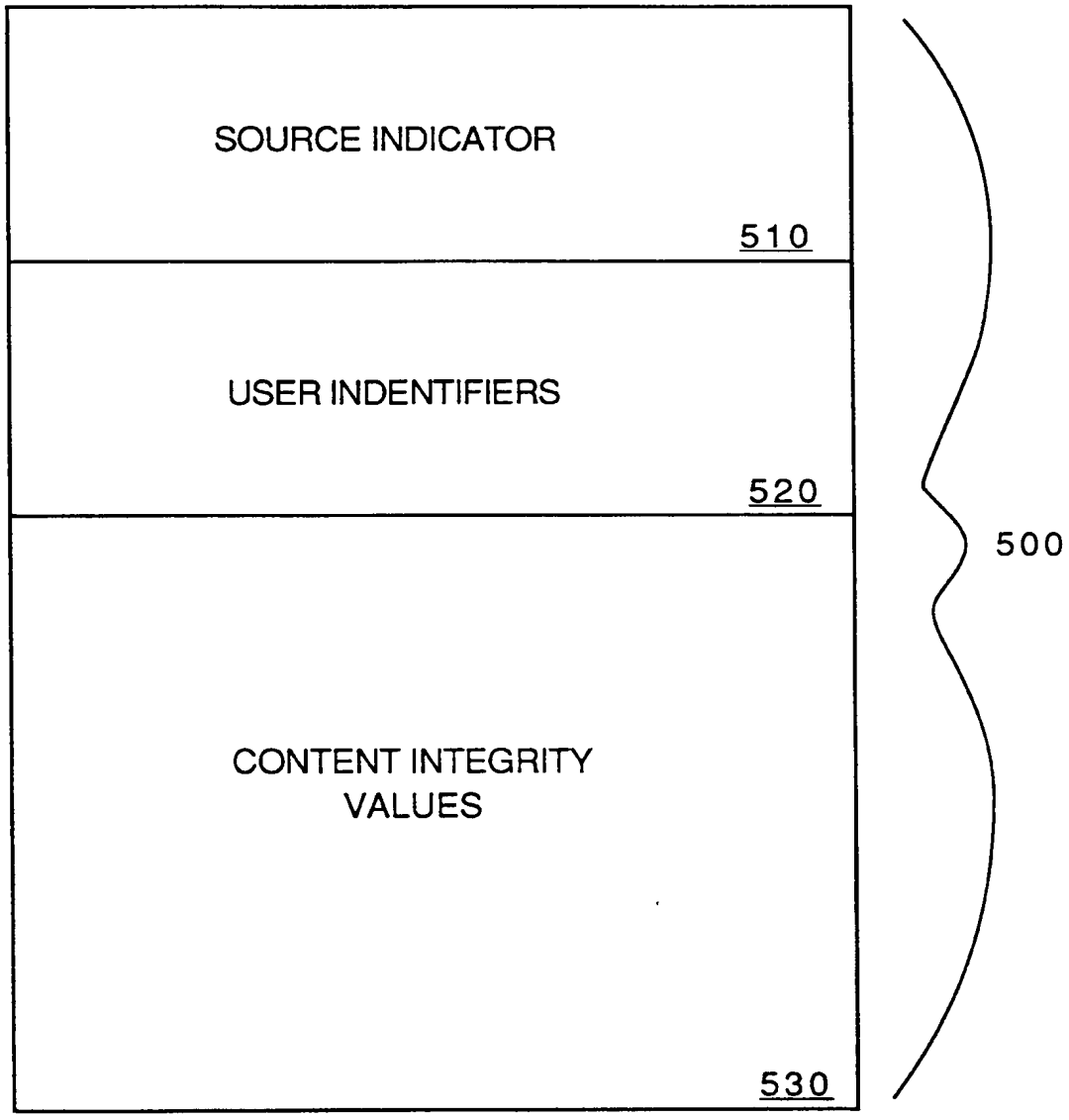

SOURCE INDICATOR
510
USER INDENTIFIERS
520
CONTENT INTEGRITY VALUES
530
500

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/31314

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 12/14
US CL : 713/200, 201, 202; 709/227, 229, 238, 250
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202; 709/227, 229, 238, 250

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

BRS/WEST, EAST, IEL ON LINE
(stream$3 or set) near5 digital! same (authoriz$5 or permit$3 or authenticat$4) and (play$3 or playback or replay$3)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,809,144 A (SIRBU et al) 15 September 1998, col. 2, line 4 to col.16, line 49.	1-22
Y	US 5,675,734 A (HAIR) 07 October 1997, col. 4, line 9 to col. 5, line 16.	1-22
A,P	US 5,966,440 A (HAIR) 12 October 1999, entire document.	1-22
A,P	US 5,926,624 A (KATZ et al) 20 July 1999, entire document.	1-22
A	US 5,734,719 A (TSEVDOS et al) 31 March 1998, entire document.	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 21 MARCH 2000	Date of mailing of the international search report 25 APR 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JOSEPH PALYS Joni Hill Telephone No. (703) 305-9685

Form PCT/ISA/210 (second sheet) (July 1998)★